B. REMARKS (COMMENTS)

A. AMENDMENTS AND SPECIFICATION AND DRAWINGS

No amendments have been requested as the drawings, or specification pursuant to the parameters of 35 U.S.C 112, etc.

C. AMENDMENTS TO CLAIMS UNDER 35 U.S.C. 101

Applicant has amended claims 1, 2, 3, and 4 pursuant to the provisions of 35 U.S.C. 101. Claims 1, 2 and 4 have each been amended in specific and different particulars so that each claim is now considered in compliance with 35 USC 101 (claims 1 and 2 are also amended pursuant to 35 USC 102 rejection). Under Clemot, all claims 1, 2, 3 and 4 have been amended pursuant to the provisions of all other references under 35 USC 102. Claim 5 is cancelled and new claim 6 is submitted.

D. REJECTION UNDER 35 U.S.C. 102

A. The examiner has rejected claims 1, 2, 3, 4, 5 based on the Clemot U.S. Patent , 5,894,519 (and other references).

Further, the Clemot reference patent does not disclose the use of means to achieve an overall code comparison by any proper mathematical or algogromithic methodology: and only incidentally refers some comparative function. This later aspect is not the intended focus of the references. As to the 35 U.S.C. 102 rejection, attention is drawn to the following additional language in the specification of Clemot.

"The object of the invention is to obviate the disadvantages of the aforementioned processes. To this end, it proposes a process for dissimulating a secret code in an authentication device, such as a floppy disk or smart card. This process makes it possible to locally check the secret code entered by the user, whilst limiting dictionary access risks".

"More specifically, the invention relates to a process for the dissimulation of a secret code in a data authentication device consisting of encrypting the secret code by an encrypting function to form a secret code image and storing said secret code image in the authentication device. This process is characterized in that it consists, beforehand, of choosing an encrypting function such that, with each secret code image corresponds a plurality of antecedent codes all differing from the secret code, but which, once encrypted by the encrypting function, have an image identical to that of the secret code".

"Advantageously, the secret code having n characters, the encryption function consists of associating with these n characters a secret code image with k characters, with k, n".

According to a preferred embodiment of the invention, the number k of characters of the image of the secret code is n/2.

"The invention also relates to a process for the checking of the secret code of a user wishing to access a central system from a terminal. As said user is provided with an authentication device in which is dissimulated the image of the secret code by the encrypting function, said process is characterized in that it comprises a stage of locally checking the secret code entered by the user and encrypted by the encrypting function, b comparison with the image of the secret code stored in the authentication device and then, if this is checked, it consists of a stage of authenticating by the central system".

Applicant maintains that the subject physical access to a system through the computer system and algorithmic means is not taught by the references. The unlocking system of applicant provides a shutoff mechanism if various attempts are made that fail as back up guard. The references do not teach this aspect.

E. CONCLUSION

In conclusion, Applicant maintains that the subject application is ready for allowance as to amended claims 1, 2, 3, 4 and new claim 6.

George R. Royer
Applicant

CERTIFICATE OF MAILING

Certification is made that the foregoing response and amendment was mailed to the commissioner of Patents and Trademarks, U.S. Patent Office, P.O. Box 1450, Alexandria, Virginia 22313-1450 with mailing being made on August 2007 by U.S. Postal Service by way of U.S. Postal Service Express Mail Number ______________________.

George R. Royer
Applicant